Amendments to the Specification:

Please replace the paragraph at page 3, lines 22 through 29 with the following amended paragraph:

An object of the present invention is to allow a sender to generate an ad-hoc public-private key pair whose ~~encrypted~~ private key is known only to the sender in order to encrypt an e-mail message to a receiver without the receiver's involvement, when there is no known receiver public key for the sender to use, or the receiver is not online to participate in a key negotiation protocol to set up a shared key with the sender, or an out-of-band shared key distribution between the sender and the receiver is not practical, or it is more secure for the sender to be able to use a public key instead of accessing a stored secret shared key to encrypt the sender's multiple messages.

Please replace the paragraph at page 4, line 20 through page 5, line 9 with the following amended paragraph:

A receiver desiring to decrypt an encrypted electronic message received from a sender authenticates the receiver to the sender; derives an index value that is uniquely associated with an ad hoc public key and private key asymmetric key pair, the key pair uniquely associated with both the sender and the receiver; retrieves an encrypted private key from a key server by utilizing the index value, the ~~encrypted~~ private key known only to the sender; and decrypts the encrypted electronic message by utilizing the encrypted private key. In an alternative embodiment, an unencrypted private key is obtained from the encrypted private key by utilizing a sender secret, and the encrypted electronic message is decrypted by utilizing the unencrypted private key. In another embodiment, the index value is known only to the sender. In an alternative embodiment, an identity value is obtained by utilizing at least a unique identification for the sender and a unique identification for the receiver, and the index value is computed from the identity value by utilizing a sender secret. In another embodiment, the electronic message is an electronic mail

message. In another embodiment, the key pair is a set of at least one key pair, each key pair associated with a validity field, and an encrypted private key is retrieved and utilized for decrypting the encrypted electronic message, the encrypted private key selected from the set based on the associated validity field. In yet another embodiment, the ad hoc public key and private key asymmetric key pair is an ad hoc symmetric key.

Please replace the paragraph at page 6, line 25 through page 7, line 3 with the following amended paragraph:

At step 202, sender server S102 salts and stretches a sender secret S103 passphrase to 256 bits long for approximately a 128-bit security level, for use to encrypt unencrypted private key K102 into an encrypted private key K103, the private key known only to sender S100. The salt used with sender secret S103 passphrase is stored alongside encrypted private key K103. The symmetric encryption functions for encrypting unencrypted private key K102 are as described later below. Public key K101 and encrypted private key K103 make up an ad hoc key pair K100 that is uniquely associated with both sender S100 and receiver R100.

Please replace the paragraph at page 10, line 13 through line 15, with the following amended paragraph:

At step 503, sender server S102 retrieves via secure channel encrypted private key K103 that is stored in key server KS101 by using index value V101, ~~encrypted~~ the private key ~~K103~~ known only to sender S100.